PCT/EP 03 / 14632
21.01.04

BUNDESREPUBLIK DEUTSCHLAND

17 JUN 2005

REC'D 06 FEB 2004
WIPO PCT

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 59 755.3

Anmeldetag: 19. Dezember 2002

Anmelder/Inhaber: BT Ingnite GmbH & Co, 80687 München/DE

Bezeichnung: Automatische Terminal- oder Nutzeridentifizierung in Netzwerken

IPC: H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 9. Januar 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Wallner

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

A 9161
06/00
EDV-L

Automatische Terminal- oder Nutzeridentifizierung in Netzwerken

Die vorliegende Erfindung bezieht sich auf eine automatische Terminal- oder Nutzeridentifizierung in Netzwerken, insbesondere im Netzverbund des Internets, und insbesondere auf ein Verfahren zum automatischen Erkennen eines Zugriffsrechts auf geschützte Bereiche in Netzwerken, insbesondere im Netzverbund des Internet, wobei der Begriff geschützter Bereich jegliche nicht frei verfügbaren Transaktionen umfasst.

Die Handhabung von sensiblen Daten oder Transaktionen unter Ausschluß Unberechtigter in Netzwerken, insbesondere im frei zugänglichen Internet stellt große Sicherheitsprobleme dar. Einerseits müssen zunächst Zugriffsrechte für die Transaktionen unter Ausschluß Unberechtigter sichergestellt werden und andererseits muss anschließend eine sichere Übertragung der Daten erfolgen. Die vorliegende Erfindung befasst sich mit dem ersten dieser Probleme, nämlich der Prüfung, ob ein Terminal, der Transaktionen unter Ausschluß Unberechtigter durchführt, auch Zugriffsrechte hierfür besitzt.

Ein übliches Verfahren zur Identifizierung eines Terminals oder Nutzers für die Lieferung einer bestimmten Leistung, wie zum Beispiel den Zugriff auf geschützte Bereiche im Internet, ist die Abfrage eines Benutzernamens und eines Passwortes. Ein solches Verfahren, bei dem ein Benutzername und Passwort abgefragt wird, sieht eine relativ hohe Sicherheit hinsichtlich der Identifizierung des Nutzers vor. Bei diesem Verfahren ist es jedoch notwendig, dass sich der Nutzer zunächst in irgendeiner Form registrieren lassen muss, um einen gewünschten Bereich zu nutzen. Dies hat für den Nutzer zur Folge, dass er ggf. persönliche Daten für die Registrierung bereitstellen muss, ohne dass ihm dies Recht wäre. Darüber hinaus schreiben sich Nutzer heutzutage häufig Benutzernamen und Passwörter nieder, da sie zu viele Passwörter oder Pins, z.B. für den Zugriff auf den eigenen Rechner, die Kontokarte, die Kreditkarte etc. verwalten müssen. Das Niederschreiben birgt jedoch bekanntermaßen ein Sicherheitsrisiko. Für den entsprechenden Anbieter des Diens-

Dienstes bedeutet dies ferner, dass eine entsprechend leistungsfähige Kundendatenverwaltung vorgesehen ist, die in der Regel manueller Pflege bedarf.

Für den Anbieter einer bestimmten Leistung ist es aber oft nicht notwendig, dass der Empfänger der Leistung sich bei ihm in irgendeiner Form registriert. So ist z.B. der Kunde beim offenen Call-by-Call oder beim offenen Internet-by-Call für den Netzbetreiber (Anbieter) anonym. Dem Netzbetreiber, sind lediglich die Anruf-Rufnummer, d.h. eine eindeutige Anschlußkennung eines ansonsten anonymen Kunden, die Zielrufnummer und die Dauer des Anrufs bekannt. Zur Abrechnung werden diese Daten in der Regel zum Inkasso an die Telefongesellschaft des Kunden, beispielsweise die Deutsche Telekom AG, übermittelt. Dabei kann der Kunde für den Anbieter einer bestimmten Leistung völlig anonym bleiben, da außer der eindeutigen Anschlußkennung keine weiteren Informationen über den Kunden erforderlich sind.

Möchte der Netzbetreiber oder Dienstanbieter dem jeweiligen Kunden jedoch Transaktionen unter Ausschluß unberechtigter Dritter Anbieten, beispielsweise vertrauliche Daten - wie einen Einzelverbindungsnachweis - zur Verfügung stellen oder den Zugriff auf andere geschützte Bereiche ermöglichen, so war dies bisher nur mit einer vorherigen Registrierung möglich, um sicherzustellen, dass nur autorisierte Terminals auf die jeweiligen Daten zugreifen können.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, eine automatische Identifizierung von Zugriffsrechten auf geschützte Bereiche in Netzwerken, insbesondere im Internet zu ermöglichen.

Erfindungsgemäß wird diese Aufgabe bei einem Verfahren zum automatischen Erkennen eines Zugriffsrechts auf geschützte Bereiche in einem ersten Netz unter Verwendung einer eindeutigen Anschlusskennung eines zweiten Netzes, insbesondere im Netzverbund des Internets, mit folgenden Verfahrensschritten: dynamische oder statische Zuordnung einer eindeutigen Kennung des ersten Netzes für einen Terminal, bei bzw. vor seinem Verbin-

dungsaufbau mit dem ersten Netz, Speichern einer Kombination aus wenigstens der eindeutigen Anschlußkennung des zweiten Netzes und der eindeutigen Kennung des ersten Netzes in einer Authentifizierungseinheit Abfragen der Authentifizierungseinheit zum Ermitteln der eindeutigen Anschlußkennung des zweiten Netzes anhand der eindeutigen Kennung des ersten Netzes, wenn der Terminal auf den geschützten Bereich zugreifen möchte, Prüfen, ob für die eindeutige Anschlußkennung des zweiten Netzes ein Zugriffsrecht für den geschützten Bereich besteht. Das vorliegende Verfahren ermöglicht somit eine sichere automatische, Erkennung von Zugriffsrechten auf geschützte Bereiche in Netzwerken anhand der Kennungen aus zwei unterschiedlichen Netzen. Eine Vorabregistrierung mittels Benutzername und Passwort sowie der Angabe persönlicher Informationen ist nicht notwendig. Aber selbst bei dem Zugriff auf Bereiche die zusätzlich eine Registrierung erfordern, wie zum Beispiel kostenpflichtige Datenbanken, ermöglicht das erfindungsgemäße Verfahren, dass der Zugriff nur von bestimmten Netzelementen insbesondere bestimmten Telefonanschlüssen (sowohl Mobil- als auch Festnetz) aus möglich ist, was einen Missbrauch selbst bei Verlust oder bewusster Weitergabe von Benutzernamen und Passwort ausschließt.

Gemäß einer bevorzugten Ausführungsform der Erfindung enthält die in der aktuellen Authentifizierungseinheit gespeicherte Kombination zusätzliche Daten, wie beispielsweise die Einwahl-Rufnummer in das Netzwerk, einen Benutzernamen (Login) und/oder ein Passwort. Diese Daten können eine noch bessere Identifizierung des Terminals ermöglichen, wobei insbesondere der Benutzername und das Passwort automatisch bei der Einwahl in das Netzwerk erzeugt werden können.

Bei einer besonders bevorzugten Ausführungsform der Erfindung wird die Authentifizierungseinheit nur temporär geführt, so dass es sich im Wesentlichen um eine dynamische Einheit handelt. Vorzugsweise wird die Kombination an Daten aus der Authentifizierungseinheit gelöscht, sobald der Terminal seine Verbindung beendet. Somit wird sichergestellt, dass ein Zugriff auf den

geschützten Bereich nur solange möglich ist, wie eine Verbindung von der eindeutigen Anschlußkennung zu dem Netzwerk besteht.

Bei einem Ausführungsbeispiel der Erfindung ist die eindeutige Kennung des zweiten Netzes eine Anrufrufnummer. Vorzugsweise umfaßt der geschützte Bereich das Bereitstellen eines Online-Einzelverbindungsnachweises, so dass der Nutzer von Call-by-Call oder Internet-by-Call Diensten auf seine Verbindungsnachweise zugreifen kann, ohne sich vorher registrieren zu müssen. Dabei erfolgt der Einzelverbindungsnachweis automatisch für die eindeutige Anschlußkennung des Terminals. Bei einer alternativen Ausführungsform der Erfindung ist vor Freigabe eines Einzelverbindungsnachweises eine weitere Eingabe am Terminal des Nutzers notwendig, um sicherzustellen, dass nicht jeder Terminal, der Zugriff auf ein Bestimmtes Netzelement bzw. einen bestimmten Telefonanschluss besitzt, auch die Verbindungsnachweise dieses Anschlusses abrufen kann. Beispielsweise umfaßt die weitere Eingabe das Eingeben einer Rechnungs- und/oder Kundennummer der Telefongesellschaft, und oder einer PIN.

Um eine hohe Sicherheit bei der Identifizierung sicherzustellen, und einen Missbrauch der Authentifizierungseinheit sicherzustellen haben nur autorisierte Dienste Zugriff auf die Authentifizierungseinheit, die sich ggf. bei der Authentifizierungseinheit vorab registrieren müssen und sich bei der Abfrage identifizieren.

Bei einer Ausführungsform der Erfindung umfaßt der geschützte Bereich wenigstens einen der folgenden Dienste: Bereitstellung von Daten (kostenpflichtige Datenbanken), elektronischer Handel (E-Commerce) und Payment. Im E-Commerce Bereich kann zwar in der Regel eine Vorabregistrierung eines Kunden nicht entfallen, aber die Nutzung der E-Commerce-Dienste kann erleichtert werden, da ein Terminal automatisch anhand seiner Anschlusskennung wie z.B. seinem Telefonanschluss, erkannt werden kann. Bei dem Payment Dienst können Geldbeträge beispielsweise über die Telefonrechnung eines Kunden abgerechnet werden, z.B. die einmalige Abrechnung eines klei-

nen Betrages für das Lesen eines bestimmten Zeitungsartikels im Internet. Die beim Payment Dienst entstehenden Kosten werden vorzugsweise automatisch über die eindeutige Anschlußkennung abgerechnet. Dabei ermöglicht das erfindungsgemäße Verfahren einen nachträglichen exakten Nachweis über den Verbindungsaufbau zwischen zwei Netzelementen, den Kontakt, die Bestellung und ggf. die Lieferung der erbrachten Leistung auch ohne Registrierung des jeweiligen Kunden.

Bei einer weiteren Ausführungsform der Erfindung werden im geschützten Bereich anhand der eindeutigen Anschlußkennung des zweiten Netzes, wie z.B. der Anschlussrufnummer oder SIM Karten Adresse, automatisch weitere Daten des Terminals aufgerufen und/oder weitere Verfahrensschritte eingeleitet. Die zusätzlichen Daten können sich beispielsweise aus einer Vorabregistrierung unter der eindeutigen Anschlußkennung ergeben. Solche zusätzlichen Daten sind insbesondere im E-Commerce Bereich zweckmäßig, wo ggf. Zustell- und Rechnungsadressen eingegeben werden müssen. Als weitere Verfahrensschritte kann z. B. eine automatische Verarbeitung einer Bestellung erfolgen. Das erfindungsgemäße Verfahren kann ferner auch in Kombination mit der bekannten Authentifizierung mit Benutzernamen und Passwort verwendet werden, um eine noch höhere Datensicherheit zu erreichen.

Die der Erfindung zugrundeliegende Aufgabe wird auch bei einem Verfahren zum Bereitstellen von Daten für eine automatische Erkennung von Zugriffsrechten auf geschützte Bereiche in Netzen, insbesondere im Netzverbund des Internets, mit folgenden Verfahrensschritten gelöst: Vorsehen von wenigstens jeweils einer eindeutigen Kennung aus wenigstens zwei unterschiedlichen Netzen während eine Verbindung zu beiden Netzen besteht, Speichern einer Kombination der unterschiedlichen Kennungen in einer dynamischen Authentifizierungseinheit, Ausgeben und/oder Authentifizieren einer der eindeutigen Kennungen, bei einer entsprechenden Anfrage hinsichtlich der anderen eindeutigen Kennungen, Löschen der Daten aus der dynamischen Authentifizierungseinheit sobald eine Verbindung mit wenigstens einem der beiden Netze beendet wurde. Das erfindungsgemäße Verfahren sieht eine dynamische Au-

thentifizierungseinheit von aktuell im Netzwerk befindlichen Terminals vor, die eine Identifizierung eines Terminals anhand seiner eindeutigen Kennung aus beiden Netzwerken ermöglicht. Dabei wird die Authentifizierungseinheit in Echtzeit geführt, sodass die gespeicherten Daten nur solange vorgehalten werden, wie der Terminal im Netzwerk ist. Nach Beenden der Verbindung werden die Daten umgehend gelöscht, um einen Missbrauch zu verhindern.

Vorzugsweise ist wenigstens eine der Kennungen eine IP-Nummer und/oder eien eindeutigen Anschlußkennung eines Terminals.

Für eine erhöhte Datensicherheit wird geprüft, dass die Anfrage hinsichtlich einer bestimmten IP-Nummer von einem autorisierten Dienst stammt. Hierdurch wird sichergestellt, dass die in der Authentifizierungseinheit befindlichen Daten nicht missbräuchlich verwendet werden.

Für eine erhöhte Datensicherheit sind in der aktuellen Authentifizierungseinheit zu der oben genannten Kombination zusätzliche Daten gespeichert. Diese können beispielsweise die Einwahl-Rufnummer, einen Benutzernamen (Login) und ein Passwort umfassen. Diese zusätzlichen Daten sehen eine noch erhöhte Identifizierungssicherheit vor.

Bei einer Ausführungsform der Erfindung kann über die Authentifizierungseinheit bzw.. die ausgegebene Kennung eine Anruf-Rufnummernsperre oder eine Ziel-Rufnummernsperre identifiziert werden.

Die vorliegende Erfindung wird nachfolgend anhand eine bevorzugten Ausführungsbeispiels der Erfindung unter Bezugnahme auf die Zeichnung näher erläutert. In der Zeichnung zeigt:

Fig. 1 eine schematische Systemübersicht für einen offenen Internet-by-Call Dienst eines Telekommunikations-Netzbetreibers.

Anhand der Fig. 1 wird das erfindungsgemäße Verfahren bei einer automatischen Erkennung von Zugriffsrechten am Beispiel eines Online Einzelverbindungsnachweises (EVN) für Internet-by-Call Kunden näher erläutert.

Zunächst wird jedoch der allgemeine Abrechnungsmodus bei einem Internet-by-Call Dienst beschrieben. Bei einem offenen Internet-by-Call Dienst wählt sich ein Kunde, dessen Anschluss beispielsweise auf die Deutsche Telekom AG (DTAG) läuft, über das Netz der DTAG in das Netzwerk eines entsprechenden Netzbetreibers, der nachfolgend als Anbieter bezeichnet wird, ein. Die DTAG vermittelt den entsprechenden Anruf in ihrem Netz bis zu einem definierten Übergabepunkt, der auch als point of interconnect (POI) bezeichnet wird. An diesem POI wird der Anruf von der DTAG an den Anbieter des Internet-by-Call Dienstes übergeben. Gegebenenfalls kommt es nun zu einer Vermittlung des Anrufs im Netz des Anbieters, und der Anruf wird auf einer Modembank des Anbieters terminiert. Sofern erforderlich, werden die Kundendaten, wie beispielsweise ein Benutzername und ein Passwort geprüft und anschließend wird dem Kunde eine (dynamische) IP-Adresse zugewiesen. Nun wird der Anruf auf Basis des Internet-Protokolls (IP) bis zu seiner Zielde-stination (z.B. dem öffentlichen Internet) weitervermittelt.

Die zur Abrechnung des Anrufs relevanten Daten werden von dem Anbieter festgehalten, und zum Inkasso an die DTAG weitergeleitet.

Der Anbieter bekommt von der DTAG Informationen hierüber, welche Datensätze auf welcher Rechnungsnummer (Rechnungsnummer, Kundennummer sowie Rechnungsdatum) abgerechnet wurden, ohne dass dem Anbieter die Personalien des Kunden bekannt sind.

Die DTAG listet auf ihren Rechnungen nicht die einzelnen Internet-by-Call Anrufe des Kunden auf, die dieser aber, wie nachfolgend beschrieben wird, Online abfragen kann.

Das nachfolgend unter Bezugnahme auf Fig. 1 beschriebene System ermöglicht eine automatische anschlussbezogene Authentifizierung eines Kunden, um den Zugriff auf einen Online-Einzelverbindungsnachweis eines Internet-by-Call Anbieters zu ermöglichen.

Block 1 in Fig. 1 stellt das Telekommunikationsnetz außerhalb des Netzwerks des Anbieters dar. Im Block 1 erfolgt somit die Einwahl und die Vermittlung des Anrufs bis zum POI des Internet-by-Call Anbieters.

Das System des Netzanbieters ist durch einen gestrichelten Kasten 2 in Fig. 1 dargestellt.

Der Block 4 in Fig. 1 repräsentiert einen Switch, in dem die zur Abrechnung des Kunden relevanten Daten erzeugt werden. Diese Kundendaten, die als Call-Data-Records (CDR) bezeichnet werden, enthalten z.B. die eindeutige Anschlußkennung des Kunden, die Einwahl-Rufnummer in das Netzwerk des Anbieters und die Start- sowie die Endzeit des Anrufs. Diese Daten werden im Netz des Anbieters zu einem Berechnungssystem im Block 6 weitergeleitet, das die Kosten für den jeweiligen Anruf berechnet. Die berechneten Kosten werden unter Angabe der eindeutigen Anschlußkennung an die DTAG im Block 8 übermittelt. Die DTAG stellt diese Kosten nachfolgend dem Kunden des jeweiligen Anschlusses der eindeutigen Anschlußkennung in Rechnung und liefert Daten betreffend die Rechnungsstellung zurück an das Berechnungssystem im Block 6. Diese Daten enthalten beispielsweise die Rechnungsnummer, die Kundennummer sowie das Rechnungsdatum. Nicht enthalten sind die persönlichen Daten des Kunden.

Vom Block 6 werden die berechneten Kosten gemeinsam mit den CDR-Daten zu einem netzinternen Datenbankserver im Block 10 übermittelt. Diese Übermittlung kann sofort oder erst nach Erhalt der Rechnungsdaten durch die DTAG erfolgen. Wenn die Übermittlung der Daten sofort erfolgt, werden die später von der DTAG zurückgesandten Rechnungsdaten nach Erhalt nach-

träglich an den Datenbankserver 10 übermittelt, welche diese Daten dann kumuliert bzw.gesteuert.

Der Switch im Block 4 leitet einen Teil der CDR-Daten, nämlich die eindeutige Anschlußkennung und die Einwahl-Rufnummer an eine Modembank im Block 12 weiter, wo der Anruf terminiert wird. Von der Modembank im Block 12 werden die Daten an einen Server im Block 14 übermittelt. Dort wird eine aktuelle IP-Adresse für den Anruf verteilt. Die aktuelle IP-Adresse, sowie die dazugehörige eindeutige Anschlußkennung und die Einwahl-Rufnummer werden anschließend an eine Authentifizierungseinheit im Block 16 weitergeleitet. Wenn der Anruf beendet ist, d.h. die Verbindung zwischen dem Netzwerk des Anbieters und dem Kunden getrennt wird, teilt der Switch im Block 4 der Modembank im Block 12 mit, dass der Anruf beendet wird. Der entsprechende Platz an der Modembank wird freigegeben, und die Modembank teilt dem Server im Block 14 unter Angabe der entsprechenden IP-Adresse mit, dass der Anruf beendet wurde. Der Server im Block 14 wiederum überträgt diese Information sofort an die Authentifizierungseinheit, in der die Daten aus IP-Adresse, eindeutiger Anschlußkennung und Einwahl-Rufnummer sofort gelöscht werden. Die Authentifizierungseinheit beinhaltet somit eine dynamische Datenbank, in der jeweils nur aktuelle Authentifizierungsdaten gespeichert sind, d.h. Daten betreffend eine aktuelle Verbindung zwischen einem Anschluss eines Kunden (eindeutigen Anschlußkennung) und einem Einwahlpunkt des Netzwerkes (Einwahl-Rufnummer) sowie die dynamisch zugewiesene IP-Adresse. Diese bestimmte Kombination an Daten wird nur solange gespeichert, wie eine tatsächliche Verbindung zu einem Anschluss des Kunden besteht.

Möchte ein Kunde nun seine Rechnungsdaten Online einsehen, so wird er im Netzwerk des Anbieters die entsprechende Internetseite, die Zugriff auf den Datenbankserver im Block 10 besitzt, über ein Webinterface im Block 20 aufrufen. Über das Webinterface wird der Datenbankserver 10 zwar die aktuell zugewiesene IP-Nummer des Kunden mitgeteilt, nicht jedoch dessen eindeutigen Anschlußkennung. Der Datenbankserver im Block 10 stellt daher eine

Anfrage an die Authentifizierungseinheit im Block 16, um festzustellen, ob die bei der Anfrage verwendete IP-Adresse des Kunden eine aktuelle IP-Adresse darstellt, und ferner, welchem Anschluss, d.h. welcher eindeutigen Anschlußkennung, die IP-Adresse zugewiesen wurde. Wenn es sich um eine aktuelle IP-Adresse handelt, wird die Datenkombination aus der Authentifizierungseinheit an den Datenbankserver im Block 10 geliefert, und der Datenbankserver kann nun die der eindeutigen Anschlußkennung zugehörigen Einzelverbindungsnachweise herausfiltern und zur Einsicht freigeben. Gegebenenfalls können auch zusätzliche Informationen, wie beispielsweise eine PIN und/oder eine Rechnungs- und/oder Kundennummer der DTAG angefordert werden, um die Information hinsichtlich des Einzelverbindungsnachweises auch nur der Person bzw. dem Terminal zur Verfügung zustellen, die bzw. der tatsächlich Zugriff auf die Rechnung der DTAG besitzt.

Das wesentliche Merkmal für eine sichere, anschlussbezogene Identifizierung eines Terminals ist das Vorsehen der dynamischen Authentifizierungseinheit, die nur Daten für aktuell bestehende Verbindungen enthält, und somit eine hohe Sicherheit gegen Missbrauch bietet.

Obwohl die vorliegende Erfindung speziell anhand eines Online Einzelverbindungsnachweises beschrieben wurde, ist die anschlussbezogene Authentifizierung von Zugriffsrechten natürlich auch auf andere Gebiete ausweitbar. Beispielsweise könnte ein beliebiger netzinterner oder auch netzexterner Dienst auf die Authentifizierungseinheit zugreifen, um festzustellen, ob und welchem Telefonanschluss (eindeutige Anschlußkennung) eine bestimmte IP-Adresse aktuell zugewiesen ist. Die eindeutige Anschlußkennung läßt nunmehr eine anschlussbezogene Authentifizierung durch den jeweiligen Dienst zu. Dabei dürfen natürlich nur bestimmte registrierte Dienste auf die Authentifizierungseinheit zugreifen, die sich auch jeweils gesondert identifizieren müssen, um einen Missbrauch der Authentifizierungseinheit zu verhindern.

Solche Dienste sind beispielsweise Payment Dienste, welche Beträge über ein entsprechendes Inkassosystem über die Telefonrechnung der DTAG ab-

rechnen. Eine derartige Abrechnung erfolgt beispielsweise beim kostenpflichtigen Lesen bestimmter Zeitungsartikel im Internet. Ein Nachweis über das Zustandekommen der Verbindung, die Bestellung, die Lieferung und somit für die Durchsetzung von Zahlungsansprüchen bzw. Lieferverpflichtungen ist somit über das obige Authentifizierungsverfahren auch bei "anonymen" Endkunden möglich.

Eine weitere Möglichkeit der Nutzung einer anschlussbezogenen Authentifizierung ist die Identifizierung durch E-Commerce Anbieter. Bei Bestellungen oder Anfragen an E-Commerce Anbieter können diese automatisch eine anschlussbezogene Authentifizierung vornehmen und somit Bestellungen eindeutig zuordnen. Dies ist insbesondere beim Kauf virtueller Produkte (z.B. Digitale Bücher, Ton- und Filmaufnahmen) Vorteilhaft, da hier die Lieferadresse keine Kontrolle darstellt. Eine weitere Authentifizierung über Benutzername und Kennwort kann dann entfallen oder zusätzlich eingesetzt werden, um eine noch höhere Sicherheit zu bieten. Anhand der anschlussbezogenen Authentifizierung kann der E-Commerce Anbieter weitere relevante Daten des Kunden aufrufen, sofern der Kunde mit der eindeutigen Anschlußkennung registriert ist.

E-Commerce Anbieter und auch Anbieter anderer Inhalte können verschiedene eindeutige Anschlußkennungen beim Netzbetreiber sperren lassen, um zu verhindern, dass weitere Transaktionen von diesen Anschlüssen aus vorgenommen werden. Insofern sieht die anschlussbezogene Authentifizierung einen Schutz gegen Missbrauch vor.

Ein weiteres Beispiel, bei dem die anschlussbezogene Authentifizierung von besonderem Nutzen sein kann, ist die Registrierung bei bestimmten Diensten über die eindeutige Anschlußkennung. Der Kunde kann beispielsweise seinen Anschluss für bestimmte Dienste freischalten lassen, und erhält daraufhin einen automatisch erzeugten Code, den er in Zukunft im Nachwahlverfahren an die Einwahl-Rufnummer anhängt. Mittels dieses Codes kann der entsprechenden eindeutigen Anschlußkennung ein bestimmter Satz an Diensten zu-

geordnet werden, die für diese eindeutige Anschlußkennung genehmigt sind (z.B. nur online-tarifierte Dienste, keine XXX-Dienste).

Auch bei einem Online-Behördengang kann der Nutzer bzw. ein Terminal sicher identifiziert werden, um Missbrauch zu vermeiden. Die anschlussbezogene Identifizierung kann in vielen Fällen eine elektronische Signatur ersetzen und ermöglicht ferner die Übertragung von aus den Telefonnetzen bekannten Zahlungsmodellen auf die Datennetze.

Die anschlussbezogene Identifizierung ermöglicht allgemein das zur Verfügung stellen von Inhalten unter Ausschluß Dritter ohne eine weitere Authentifizierung sowie das Sperren von Inhalten für eine eindeutige Anschlußkennung. Anhand der anschlusstechnischen Information lässt sich ferner überprüfen, ob eine bestimmte Leistung für diesen Anschluss sinnvoll ist. So macht es keinen Sinn, einen Videostream auf ein GSM-Handy zu übertragen, während dies für ein UMTS Endgerät oder einen Festnetzanschluss mit Terminal durchaus sinnvoll sein kann.

Die vorliegende Erfindung ist nicht auf das konkret ausgeführte Ausführungsbeispiel und die oben genannten Beispiele beschränkt. Vielmehr sieht sie allgemein eine automatische Authentifizierung eines Terminals in Netzwerken, insbesondere im Netzverbund des Internets vor, bei der wenigstens zwei Kennungen aus wenigstens zwei unterschiedlichen Netzen eingesetzt werden. Die Authentifizierung kann für verschiedene Zwecke eingesetzt werden.

Patentansprüche

1 Verfahren zum automatischen Erkennen eines Zugriffsrechts auf geschützte Bereiche in einem ersten Netz unter Verwendung einer eindeutigen Anschlusskennung eines zweiten Netzes, insbesondere im Netzverbund des Internets, mit folgenden Verfahrensschritten:

- dynamische oder statische Zuordnung einer eindeutigen Kennung des ersten Netzes für einen Terminal, bei bzw. vor seinem Verbindungsaufbau mit dem ersten Netz;
- Speichern einer Kombination aus wenigstens der eindeutigen Anschlußkennung des zweiten Netzes und der eindeutigen Kennung des ersten Netzes in einer Authentifizierungseinheit;
- Abfragen der Authentifizierungseinheit zum Ermitteln der eindeutigen Anschlußkennung des zweiten Netzes anhand der eindeutigen Kennung des ersten Netzes, wenn der Terminal auf den geschützten Bereich zugreifen möchte;
- Prüfen, ob für die eindeutige Anschlußkennung des zweiten Netzes ein Zugriffsrecht für den geschützten Bereich besteht.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die in der aktuellen Authentifizierungseinheit gespeicherte Kombination zusätzlich weitere Daten enthält.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die zusätzlichen Daten wenigstens eines der folgenden aufweisen: die Einwahl-Rufnummer in das erste Netzwerk, einen Benutzernamen (Login) und ein Passwort.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Authentifizierungseinheit nur temporär geführt wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Kombination an Daten aus der Authentifizierungseinheit gelöscht wird, sobald der Terminal seine Verbindung mit einem der beiden Netze beendet.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die eindeutige Kennung des zweiten Netzes eine Anrufrufnummer ist.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der geschützte Bereich das Bereitstellen eines Online Einzelverbindungsnachweises umfaßt.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass ein Einzelverbindungsnachweis automatisch für die eindeutige Anschlußkennung des zweiten Netzes erfolgt.

9. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass vor Freigabe eines Einzelverbindungsnachweises zusätzliche eine weitere Eingabe am Terminal notwendig ist.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass die weitere Eingabe das Eingeben einer Rechnungsnummer und/oder einer Kundennummer und/oder einer PIN umfaßt.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass nur autorisierte Dienste Zugriff auf die Authentifizierungseinheit haben.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der geschützte Bereich wenigstens einen der folgenden Dienste beinhaltet: Bereitstellen von Inhalten, elektronischer Handel (E-commerce), Payment bzw. Zahlungsdienste und Behördendienste.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass bei einem Payment Dienst die entstehenden Kosten automatisch über die eindeutige Anschlußkennung des zweiten Netzes abgerechnet werden.

14. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass im geschützten Bereich anhand der eindeutigen Anschlußkennung des zweiten Netzes automatisch weitere Daten des Terminals aufgerufen werden und/oder weitere Verfahrensschritte eingeleitet werden.

15. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine weitere Personalisierung des Terminals über die Eingabe einer PIN erfolgt.

16. Verfahren zum Bereitstellen von Daten für eine automatische Erkennung von Zugriffsrechten auf geschützte Bereiche in Netzen, insbesondere im Netzverbund des Internets, mit folgenden Verfahrensschritten:
- Vorsehen von wenigstens jeweils einer eindeutigen Kennung aus wenigstens zwei unterschiedlichen Netzen während eine Verbindung zu beiden Netzen besteht;
- Speichern einer Kombination der unterschiedlichen Kennungen in einer Authentifizierungseinheit;
- Ausgeben und/oder Authentifizieren einer der eindeutigen Kennungen, bei einer entsprechenden Anfrage hinsichtlich der anderen eindeutigen Kennungen;
- Löschen der Daten aus der Authentifizierungseinheit sobald eine Verbindung mit wenigstens einem der beiden Netze beendet wurde.

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass wenigstens eine der Kennungen eine IP-Nummer und/oder eine eindeutige Anschlußkennung eines Terminals ist.

18. Verfahren nach Anspruch 16 oder 17, dadurch gekennzeichnet, dass geprüft wird, ob die Anfrage von einer autorisierten Stelle bzw. einem autorisierten Dienst stammt.

19. Verfahren nach einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, dass die in der aktuellen Authentifizierungseinheit gespeicherte Kombination zusätzlich weitere Daten enthält.

20. Verfahren nach Anspruch 19, dadurch gekennzeichnet, dass die zusätzlichen Daten wenigstens eines der folgenden aufweisen: eine Einwahl-Rufnummer in eines der Netze, einen Benutzernamen (Login) und ein Passwort.

21. Verfahren nach einem der Ansprüche 16 bis 20, dadurch gekennzeichnet, dass über die Authentifizierungseinheit eine Anruf-Rufnummernsperre oder eine Ziel-Rufnummernsperre identifiziert wird.

Fig. 1